14741

Monge, Elaine (SCA)

From: noreply@formstack.com
Sent: Saturday, March 16, 2019 4:06 PM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

formstack

Formstack Submission For: Security Breach Notifications - With Addresses

Submitted at 03/16/19 4:06 PM

Business Name:	Upright Law
Is the business located in the United States?:	Yes
Business Address:	79 W. Monroe Street, 5th Floor Chicago, IL 60603
Foreign Business Address:	
Company Type:	Commercial
Your Name:	Colin Battersby
Title:	Counsel
Contact Address:	McDonald Hopkins, PLC 39533 Woodward Ave., Ste. 318 Bloomfield Hills, MI 48304
Contact Address:	
Telephone Number:	(248) 593-2952
Extension:	

RP

Email Address:	cbattersby@mcdonaldhopkins.com
Relationship to Org:	Other
Breach Type:	Electronic
Date Breach was Discovered:	12/27/2018
Number of Massachusetts Residents Affected:	66
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	Upright Law was recently informed by a third-party vendor that the vendor's own investigation concluded that a database hosted by the vendor and containing Upright Law's clients' personal information was potentially acquired by an unauthorized individual between July 27 and July 30, 2018. Upright Law immediately worked to determine what information was contained in the affected database in consultation with external data privacy and cybersecurity professionals experienced in handling these types of incidents. On December 27, 2018, Upright Law determined that the database contained the affected residents' full names and either their Social Security numbers, their debit account information, or both. Credit monitoring was provided to the residents whose social security numbers were impacted.
Please select the type of personal information that was included in the breached data.:	Social Security numbers = Selection(s) Credit/Debit Card Number = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	Yes

Network configuration of breached system:	Internet Access Available
For breaches involving electronic systems, complete the following:	Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)
Does your business maintain a Written Information Security Program (WISP)?:	Yes
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	Option1 | E-mail Option2 | US Mail
Please explain your answer of Other Above:	
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	01/25/2019
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services.:	No
If the breach of security includes a Social Security number, Massachusetts law requires your credit monitoring comply with Section 3A of Chapter 93H:	
Law enforcement has been notified of this data breach.:	No
Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another	Though this incident did not result from a compromise of Upright Law's systems, since the incident, Upright Law has enhanced password protocols by requiring the use of strong passwords. It is requiring two-factor authentication on new

similar breach from occurring, including updating your WISP.:	computers or devices. It has met with the vendor that was victimized here to ensure all firm data is secure and maintained in a secure environment, and is examining vendor contracts to further address security. It is also in the process of developing a formal training program for onsite staff and firm attorneys regarding information security.
Yes / No:	Yes
File 1 Upload:	View File
File 2 Upload:	
File 3 Upload:	
File - 4 Upload:	

Formstack, 11671 Lantern Road, Suite 300, Fishers, IN 46038

UPRIGHT®
LAW

14741

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted] :

I am writing with important information regarding a recent security incident. The privacy and security of the personal information provided to us is of the utmost importance to UpRight Law. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

We recently learned that an unauthorized individual may have acquired your full name, Social Security number, and debit account information. To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Because your debit account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to protecting the privacy of personal information provided to us and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with personnel familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 am to 9 pm, Eastern Time.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at [redacted]
or call [redacted] to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [redacted] for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted]

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call [redacted] or request your free credit reports online at [redacted] Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Obtaining a Police Report.

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.